UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF VERMONT

UNITED STATES OF AMERICA	:	
	:	
v.	:	Case No. 2:23-cr-34
	:	
OTMANE KHALLADI	:	

OPINION AND ORDER

Defendant Otmane Khalladi is charged in a two-count indictment with conspiracy to commit wire fraud and money laundering. Pending before the Court are three motions to suppress evidence as unreasonable searches and seizures under the Fourth Amendment. ECF Nos. 36, 37, 51. For the reasons set forth below, those motions are denied.

I. General Background

The Government alleges that Khalladi participated in a conspiracy to defraud older individuals in Vermont and elsewhere. ECF No. 36 at 2. The scheme reportedly worked as follows:

> The callers typically posed as a member of the victim's family who claimed — falsely — to have been in a significant vehicle accident resulting in potential criminal liability. A second person posing as an "attorney" representing the family member would then state that the victim would need to provide a large sum of cash, ranging from $7,000 to $30,000 to bail the family member out of jail.... [T]he victims were often instructed to provide the money to a "bail bondsman" and also instructed that the victim must not discuss the case with anyone because of a "gag order."

Id. at 2-3. On October 19, 2022, Khalladi was charged with international money laundering and international money laundering conspiracy in the Northern District of New York. ECF No. 43 at 2. He made an initial appearance on December 13, 2022, and was ordered released pursuant to pretrial conditions. *Id.* One of those conditions required him to remain at an authorized address as approved by Pretrial Services, which was an apartment at 805 South Miami Avenue in Miami, Florida. *Id.*

On April 6, 2023, a federal grand jury in this District returned a two-count indictment charging Khalladi with wire fraud conspiracy and money laundering conspiracy. *Id.* An arrest warrant was issued in conjunction with the indictment. *Id.* The grand jury investigation "involved multiple witnesses who describe[d] how they conspired with Khalladi to commit the charged offenses." ECF No. 42 at 2. Those witnesses reported, among other things, that Khalladi traveled across the country in furtherance of the scheme, collecting vast sums of money. *Id.*

Pending before the Court are three motions to suppress. The first pertains to the search of a cell phone seized at the time of Khalladi's arrest in Florida. Khalladi argues that after the phone was seized, the Government waited too long to obtain a warrant. The second motion seeks suppression of information gained pursuant to a series of third-party

subpoenas, arguing that the aggregated information constituted an impermissible search.

The third motion contests two separate warrants: the first authorizing the search of specific email and iCloud accounts, and the second allowing a search for location information using one of Khalladi's cell phone numbers. Khalladi argues that the warrants did not establish probable cause because they did not show the required nexus between the places to be searched and the alleged offenses. The Government responds that the warrants were supported by the affiant's factual assertions and expertise, and that in any event the searches qualify for the good faith exception. These two latter warrants were each issued in the Western District of Oklahoma.

II. Search of Cell Phone Seized Incident to Arrest

A. Background

Khalladi's first motion to suppress alleges an unconstitutional delay in seeking a search warrant for the contents of his phone. ECF No. 36. On April 10, 2023, Homeland Security Investigations ("HSI") Special Agent ("SA") Paul Altenburg obtained a search warrant for "prospective and historical location information associated with Khalladi's iPhone." *Id.* at 3. The next day, SA Altenburg obtained a search warrant in the Southern District of Florida for

Khalladi's phone "if seized at 805 South Miami Avenue," the address authorized by Pretrial Services. *Id.*

Law enforcement officers executed the warrants the following day. Although they did not find Khalladi at 805 South Miami Avenue, another individual in the residence informed them that Khalladi could likely be found at a different residence: 25 Northeast 5th Street. ECF No. 55 at 21. Officers searched that residence, arrested Khalladi, and seized his iPhone incident to the arrest. ECF No. 43 at 3. The phone was immediately transferred to HSI-Miami's headquarters so that officers could maintain the device in a "powered-on state" inside a faraday cage (a special container that prevents electronic signals from being sent to a device "in order to prevent remote wiping of the device"). *Id.* at 11-12.

The Vermont-based officials involved in the search returned to Vermont on April 14, 2023. *Id.* at 3. SA Altenburg and Assistant United States Attorney ("AUSA") Nathanael Burris both had vacations planned beginning April 22, 2023. *Id.*; *see also* ECF No. 55 at 27. Nonetheless, Agent Anders Ostrum reached out to AUSA Burris on April 25, 2023 to ask whether a follow-up search warrant was needed for Khalladi's phone. Gov't Exhibit 6, Bates No. 4446.02. Burris indicated that he had been unaware the phone was seized incident to arrest, as he previously

believed the phone was seized pursuant to the search warrant for the phone at 805 South Miami Avenue. *Id.* at Bates No. 4446.

Agent Ostrum began working on a warrant application that same day. Gov't Exhibit 7, Bates No. 4450. He reached out to HSI agents in Miami that evening, asking for information regarding Khalladi's phone including a picture of the phone and a description of how it was seized. Gov't Exhibit 13, Bates No. 4454.02. Agent Andrea Randou responded the same day stating that both she and another Miami agent involved in Khalladi's case were away on assignment until the following week. *Id.*; *see also* ECF No. 55 at 36. The next day, April 26, Agent Ostrum again wrote to Agent Randou listing five categories of information the Vermont agents needed for the warrant application. Gov't Exhibit 12, Bates No. 4457. Agent Randou responded on May 3, copying HSI Agent Kevin Selent and stating that Agent Selent would be "better suited to answer the majority of these questions." *Id.*

On May 4, Agent Selent provided the relevant responses. Gov't Exhibit 13, Bates No. 4454. Agent Ostrum immediately followed up with "[a] few more questions," and Agent Selent responded that same day. Agent Ostrum sent a finalized search warrant affidavit to AUSA Burris later that day. Gov't Exhibit 15, Bates No. 4440.

Khalladi posted bond and was released on May 2, 2023. ECF No. 43 at 4. According to the Government, he did not request return of his phone. *See* ECF No. 43 at 9; *see also* ECF No. 55 at 55 (Agent Ostrum stating that Khalladi had not requested return as of the date of the hearing).

The Government determined that it would be easier and faster to execute the search warrant in Vermont rather than Florida. *See* ECF No. 55 at 43. Accordingly, it needed to ship Khalladi's phone to Vermont, but feared that the phone might either run out of battery or be electronically wiped in transit. *Id.* at 45-46. Because of this concern, on Friday, May 5, the Miami agents asked the Vermont agents to send them a faraday bag. Gov't Exhibit 16, Bates No. 4466. The bag was shipped to Miami on Monday, May 8. Gov't Exhibit 18, Bates No. 4444. The following Monday, May 15, HSI Miami mailed the phone back to Vermont via overnight mail. Gov't Exhibit 21, Bates No. 4473. It arrived in Vermont on Wednesday, May 17. Magistrate Judge Doyle issued a warrant the following day. ECF No. 43 at 4.

B. Analysis

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const., amend. IV. Generally, law enforcement must obtain a warrant based on probable cause in order to search or seize property. However,

if there is probable cause to believe that the property "contains contraband or evidence of a crime and if it is necessary to seize or secure the property immediately to prevent its destruction or disappearance, the Fourth Amendment allows the police to seize or secure the property without a warrant provided that they follow up by applying to a judge for a warrant to search the property's contents." *United States v. Smith*, 967 F.3d 198, 205 (2d Cir. 2020) (citing *Illinois v. McArthur*, 531 U.S. 326, 332-34 (2001)). The Supreme Court has upheld temporary seizures supported by probable cause "while the police diligently obtained a warrant in a reasonable period of time," *McArthur*, 531 U.S. at 334, and the Second Circuit has explained that "even a seizure based on probable cause is unconstitutional if police act with unreasonable delay in securing a warrant," *United States v. Martin*, 157 F.3d 46, 54 (2d Cir. 1998).

The Second Circuit expounded upon this "unreasonable delay" rule in *Smith*. In that case, an officer seized a personal tablet computer and waited 31 days to apply for a search warrant. The Second Circuit ultimately concluded that the delay was unreasonable, and therefore unconstitutional, but declined to apply the exclusionary rule "because the error by the police was due to isolated negligence and because an objectively reasonable officer would not have known in light of existing

precedent that the delay violated the Fourth Amendment." *Id.* at 202.

Smith explained that four factors are generally relevant to whether police have waited an unreasonable amount of time before obtaining a search warrant: "[1] the length of the delay, [2] the importance of the seized property to the defendant, [3] whether the defendant had a reduced property interest in the seized item, and [4] the strength of the state's justification for the delay." 967 F.3d at 206. Applying those four factors to the delay in this case, the first weighs in favor of Khalladi. *Smith* explained that "a month-long delay well exceeds what is ordinarily reasonable." *Id.* at 207. Here, the Government appears to have had most of the information required to apply for a warrant at the time of the seizure. Indeed, it had already obtained a warrant to search the phone (if it had been recovered at the 805 South Miami Avenue address). The weight of this factor is somewhat mitigated, however, by the fact of the earlier warrant since, unlike the computer in *Smith*, the Government had already shown probable cause and received permission to conduct a search.

The second factor weighs in favor of the Government. While both the Supreme Court and the Second Circuit have emphasized the "extraordinary characteristics" of personal electronic devices that entitle them to special Fourth Amendment

protection, *id.* at 207-08 (citing *Riley v. California*, 573 U.S. 373 (2014)), the *Smith* court concluded that the tablet in that case had diminished importance because (1) the defendant did not testify to its specific importance to him; (2) he had alternative electronic devices; and (3) he did not request its return, *id.* at 208. The same analysis applies here, as the Government represents that Khalladi owned multiple phones and did not request the return of this particular phone. *See* ECF No. 43 at 9; ECF No. 55 at 55. Moreover, Khalladi was incarcerated for much of the 36-day pre-warrant window, and "inability to possess or use the cell phones while incarcerated significantly diminishe[s] the importance of their prompt return." *United States v. Corbett*, No. 20-CR-213 (KAM), 2021 WL 4480626, at *5 (E.D.N.Y. Sept. 30, 2021).

Khalladi argues that he has an important privacy interest in the phone because the phone's home screen depicts his daughter. ECF No. 36 at 10. The presence of a personal photograph on a lock screen, however, does not significantly elevate the unique importance of a device.

The third factor – whether the defendant had a reduced property interest – also weighs in favor of the Government. Khalladi was arrested based on probable cause. While the phone was initially seized incident to that arrest, and not pursuant to a warrant, the Court again finds it significant that the

Government had previously obtained a warrant for the phone based upon the reasonable expectation that Khalladi would be residing at his court-approved address. *See* Gov't Exhibit 6, Bates No. 4446.02 (AUSA Burris assuming the phone had been seized pursuant to the previously issued warrant); Gov't Exhibit 4, Bates No. 1755.04 (authorizing search and seizure of electronic information stored at Khalladi's residence). Although Khalladi relinquished the phone involuntarily after his arrest for failure to comply with his conditions of release, he would have been equally obliged to surrender the phone pursuant to the earlier warrant if he had complied with those conditions.

Finally, the fourth factor weighs in favor of the Government. In *Smith*, the Second Circuit found it notable that police did not engage in "any investigation of Smith's case for nearly four weeks." 967 F.3d at 210. Here, law enforcement worked for several weeks soon after Khalladi's arrest to prepare a follow-up warrant application and to transfer the phone from Florida to Vermont. *See* ECF No. 43 at 3-4; 11. This process was delayed in part because two Miami agents were out of Florida working on other cases, and in part because law enforcement had to locate and transport a faraday bag "in order to prevent remote wiping of the device." *Id.* at 11-12.

Contrary to Khalladi's representations, investigating agents did not "simply put the issue on the back burner." ECF

No. 36 at 12. The Government actively pursued support for the warrant application as soon as it realized that the phone had not been seized pursuant to the initial search warrant. The Court concludes that any delays were justified, and not the result of neglect by the Government.

Because the *Smith* factors weigh in the Government's favor, Khalladi's first motion to suppress (ECF No. 36) is denied.

III. Third-Party Subpoenas

A. Background

To corroborate witness accounts of the conspiracy, the Government issued subpoenas to a host of companies where Khalladi had accounts. ECF No. 37 at 2. The companies included airlines and car rental agencies, phone service providers, and FedEx. ECF No. 37 at 3-6; *see also* ECF No. 37-1 (outlining 26 subpoenas to various companies for various accounts). Khalladi now asks the Court to suppress "all evidence recovered as a result of" those subpoenas. ECF No. 37 at 1-2. The central issue is whether the Government's use of subpoenas to aggregate information from 26 different sources required a warrant under the Fourth Amendment.

B. Analysis

As the First Circuit recently explained, if an individual does not have a reasonable expectation in the place to be searched "the government may use a subpoena to acquire records

in its investigation without the need of a court order based on probable cause." *United States Dep't of Just. v. Ricco Jonas*, 24 F.4th 718, 734 (1st Cir.), *cert. denied sub nom. Program Adm'r of the New Hampshire Controlled Drug Prescription Health & Safety Program v. Dep't of Just.*, 143 S. Ct. 207 (2022) (citing *Carpenter v. United States*, 585 U.S. 296, 319 (2018)). In *United States v. Miller*, the Supreme Court held that the government may subpoena bank records without a warrant.[1] 425 U.S. 435, 443-44 (1976). This gave rise to the "third party doctrine," which "stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another." *Carpenter*, 585 U.S. at 314. The Supreme Court opined in *Carpenter* that the "government will be able to use subpoenas to acquire records in the overwhelming majority of investigations." *Id.* at 319.

Carpenter noted that "pervasive tracking," such as historical cell-site location information ("CSLI"), raises special Fourth Amendment concerns because the information

[1] Khalladi implores the Court to reject *Miller* as bad law. ECF No. 37 at 14. However, he acknowledges that *Miller* "arguably remain[s] the law of the land." *Id.* The Court is bound by Supreme Court precedent. Additionally, even if the Court were to conclude that *Miller* has been tacitly overruled, it would also have to conclude that the Government reasonably relied on *Miller* as good law when collecting information pursuant to the subpoenas, and accordingly would impose the good faith exception to the exclusionary rule. *Davis v. United States*, 564 U.S. 229, 238 (2011).

preserves "a detailed and comprehensive record of the person's movements." *Id.* at 309. Khalladi argues that the Government's 26 subpoenas effectively amounted to such "pervasive tracking." The *Carpenter* Court made clear, however, that its decision was "a narrow one," and that it was not addressing "other business records that might incidentally reveal location information." *Id.* at 316. Moreover, the information obtained from the subpoenas in this case, including bank and travel records, was not nearly as "detailed and comprehensive" as CSLI, which has the "capability to pinpoint a phone's location within 50 meters." *Id.* at 313.

Khalladi compares this case to *United States v. Jones*, in which the Supreme Court held that attachment of a GPS tracking device to a vehicle and use of that device to monitor the vehicle's movement constituted an unreasonable search. 565 U.S. 400, 413 (2012). *Jones* is also distinguishable, since Khalladi's example – records obtained from a car rental company showing when his car went through certain toll locations, ECF No. 37 at 7 – simply paints a broad picture of his movements on interstate highways, and does not pin him to specific establishments such as "the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, [or] the gay bar."

565 U.S. at 415 (Sotomayor, J., concurring) (quoting *People v. Weaver*, 12 N.Y.3d 433, 551-42 (2009)).

The Court finds that each subpoena at issue was valid under the third-party doctrine, as Khalladi had no reasonable expectation of privacy in the records being sought. *See, e.g.*, *Miller*, 425 U.S. at 444 (subpoenas to banks for bank records do not violate the rights of clients of the bank); *Smith v. Maryland*, 442 U.S. 735, 742 (1979) (no reasonable expectation of privacy in phone numbers dialed because those numbers are shared with phone service providers); *United States v. Goree*, 47 F. App'x 706, 712 (6th Cir. 2002) (no reasonable expectation of privacy in airline records); *United States v. Brown*, 627 F. Supp. 3d 206, 225 (E.D.N.Y. 2022) ("[T]he third-party doctrine applies to the rental car GPS location data in this case."). The broad picture painted by the aggregation of information was not equivalent to the sort of precise data captured in either *Carpenter* or *Jones*.[2] The issuing of 26 subpoenas constituted diligent law enforcement work – not an unlawful search. Khalladi's motion to suppress the information gathered by means of the various subpoenas (ECF No. 37) is denied.

[2] Khalladi "acknowledges that courts have declined to expressly endorse th[e] ... mosaic theory" that would favor Fourth Amendment protection for aggregated searches. ECF No. 37 at 11 n.8 (citing *United States v. Tuggle*, 4 F.4th 505 (7th Cir. 2021)).

IV. Email and iCloud Account Search

A. Background

In August 2022, SA Mark Bragg applied to the United States District Court for the Western District of Oklahoma for a warrant allowing access to an email account used by Khalladi, as well as records of an iCloud account related to that email address. The affidavit supporting the warrant described the national scale of the alleged fraud, described evidence of cell phone use in the course of that fraud, and provided evidence allegedly linking Khalladi to the conspiracy. The affidavit also described information commonly stored by Apple related to iCloud accounts, including messages, voicemails, and call histories. The email address was obtained from Bank of America and the Encore Boston Harbor Resort.

With respect to evidence of Khalladi's criminal activity, SA Bragg attested that a co-conspirator had revealed he was recruited by "Otamani" or "OT" (an approximation of Khalladi's first name and his nickname, respectively). Another co-conspirator indicated that he had been provided with an iPhone for the purpose of coordinating his work as a courier. Phone records revealed that a number previously associated with that iPhone was used to contact individuals associated with Khalladi.

Law enforcement was in possession of information from Bank of America showing that Khalladi used the email account

"ot_thegoat@icloud.com" in or around August 2020. Khalladi used that same email to register for a membership card at Encore Boston Harbor Resort, a casino. The affidavit did not state when the email was used at the casino, but noted that the membership was active through at least June 2022. SA Bragg next attested that, based upon his training and experience, "@icloud.com" email addresses are commonly linked to Apple iCloud accounts, and that people generally use the same iCloud account for multiple years. He requested, and received, a warrant to search information held by Apple associated with the email account for the time period between January 1, 2022 and the date of the August 2022 affidavit.

B. Analysis

Khalladi argues that SA Bragg's affidavit did not link the email address to any criminal activity, and that the warrant therefore lacked probable cause to access either the email or the related iCloud account. The Government claims the warrant was sufficient, and argues in the alternative for application of the good faith exception.

"[A] court reviewing a challenged warrant — whether at the district or appellate level — 'must accord considerable deference to the probable cause determination of the issuing magistrate [judge].'" *United States v. Clark*, 638 F.3d 89, 93 (2d Cir. 2011) (quoting *Walczyk v. Rio*, 496 F.3d 139, 157 (2d

Cir. 2007)). "The task of the issuing magistrate [judge] is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, ... there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). A reviewing court need only ensure that the magistrate judge had a "substantial basis" for concluding that probable cause existed. *Id.* at 236.

To show probable cause, a search warrant must "establish[ ] a sufficient nexus between the criminal activities alleged" and the place or object to be searched. *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004); *see United States v. Travisano*, 724 F.2d 341, 345 (2d Cir. 1983) ("To establish probable cause to search a residence, two factual showings are necessary — first, that a crime was committed, and second, that there is probable cause to believe that evidence of such crime is located at the residence."). Probable cause to believe the suspect has committed a crime is not enough. *See United States v. Lauria*, 70 F.4th 106, 130 n.14 (2d Cir. 2023) ("this court has cautioned against confusing a fair probability that contraband or evidence of a crime will be found in a particular place with probable cause to think that the person whose premises are to be searched is implicated in the crime") (quotations omitted)). The "required nexus between the items sought and the 'particular

place' to be searched protects against the issuance of general warrants, instruments reviled by the Founders who recalled their use by Crown officials 'to search where they pleased.'" *Clark*, 638 F.3d at 94 (*quoting Stanford v. State of Texas*, 379 U.S. 476, 481 (1965)).

While "[a] showing of nexus does not require direct evidence and may be based on reasonable inference from the facts presented based on common sense and experience," *Singh*, 390 F.3d at 182, the affiant must still connect the object of the warrant to criminal conduct such that a judge can find a "fair probability" that evidence will be found, *Gates*, 462 U.S. 213, 238. As the Second Circuit stated in *Lauria*, the probable cause standard "does not demand 'hard certainties,' but it does require more than a 'hunch,' the latter being insufficient to support even an investigative stop." 70 F.4th at 128 (quoting *Gates*, 462 U.S. at 231); *see also United States v. Garlick*, No. 22-CR-540 (VEC), 2023 WL 2575664, at *6 (S.D.N.Y. Mar. 20, 2023) (holding that a warrant application must contain "enough case-specific evidence to nudge [an officer's] training and experience across the line from sheer speculation to probable cause"). "Permitting a search warrant based solely on the self-avowed expertise of a law-enforcement agent, without any other factual nexus to the subject property, would be an open invitation to vague warrants authorizing virtually automatic

searches of any property used by a criminal suspect." *United States v. Guzman*, No. S5 97 CR 786 (SAS), 1998 WL 61850, at *4 (S.D.N.Y. Feb. 13, 1998).

Here, the Government argues the Magistrate Judge had a substantial basis to find probable cause. SA Bragg's affidavit offered various grounds for believing that Khalladi was a conspirator in a wide-ranging criminal enterprise. Access to Khalladi's email and the related iCloud account offered law enforcement a potentially significant opportunity to uncover evidence of that scheme. *See Lauria*, 70 F.4th at 130 ("probable cause as to a person's criminal conduct can sometimes inform probable cause to search a place used or frequented by that person or to obtain records for electronic devices linked to that person").

Nonetheless, the affidavit provided no basis to believe that the email address in question was ever used for, or in relation to, criminal activity. There was no suggestion of criminal conduct related to either Bank of America or the Encore Boston Harbor Resort – the two entities that reported use of the email address. Nor was there any evidence that the email account had been used during the period under investigation. Of the 33 factual paragraphs in SA Bragg's affidavit, only the final paragraph offered any information about the account, identifying the sources of the information and the account's

last known date of use. SA Bragg offered no opinion, aside from his conclusion as to probable cause, about the likely use of the email account in the criminal conspiracy. The affidavit instead stated that @icloud.com emails are linked to Apple iCloud accounts, and that people often use the same iCloud account for years.

"[A] law enforcement officer's professional opinion, and any reasonable inferences that may be gleaned from it, must be considered in tandem with the actual, particularized facts sworn in the search affidavit regarding the place or item to be searched." *United States v. Santos*, No. 23-CR-436 (OEM), 2024 WL 3566983, at *9 (E.D.N.Y. July 29, 2024). In *Santos*, the court noted that "crucially missing" from the agent's affidavit was "any averred factual connection between Santos' cellphone and any purported use, by Santos, of a cellphone in connection with either robbery and theft." *Id.* at *10. Similarly, in *United States v. Garcia* the court found that where "the affidavit merely alleged facts supporting an inference that Garcia committed the crime, but provided no factual basis whatsoever to believe that evidence of that crime would be found on Garcia's cell phone, there is not a substantial basis for the issuing judge to conclude that there was probable cause to search the phone." No. 3:20-CR-00058 (KAD), 2023 WL 4850553, at *7 (D. Conn. July 28, 2023).

An affidavit seeking a warrant to search an email account "do[es] not have to provide specific evidence that every category of evidence sought will be present in that ... account, but can rely on the affiant[']s] training, experience, and the totality of the circumstances to support a 'common-sense' probability that the evidence may be found there sufficient for probable cause." *United States v. Pinto-Thomaz*, 352 F. Supp. 3d 287, 306 (S.D.N.Y. 2018). Here, with no facts linking the email account to criminal activity and no relevant expert input from the agent, the totality of circumstances did not provide a "substantial basis" for concluding that probable cause existed. *Gates*, 462 U.S. at 236. Absent the necessary nexus between the alleged criminal enterprise and the email and iCloud accounts in question, the Court finds that the warrant failed to establish probable cause.

That said, a warrant issued in "violation of the Fourth Amendment does not necessarily result in the application of the exclusionary rule." *United States v. Rosa*, 626 F.3d 56, 64 (2d Cir. 2010). In *United States v. Leon*, the Supreme Court recognized an exception to the exclusionary rule for "evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant." 468 U.S. at 922. The Court reasoned that, in those circumstances, "[p]enalizing the officer for the magistrate [judge's] error, rather than his own, cannot

logically contribute to the deterrence of Fourth Amendment violations." *Id.* at 921. "The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance" on an invalidated warrant. *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992).

The Supreme Court has identified four circumstances where the good faith exception to the exclusionary rule applies:

> (1) where the issuing magistrate [judge] has been knowingly misled; (2) where the issuing magistrate [judge] wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.

United States v. Moore, 968 F.2d 216, 222 (2d Cir. 1992) (citing *Leon*, 468 U.S. at 923); *see Clark*, 638 F.3d at 100. Here, Khalladi does not argue that the issuing judge abandoned his judicial role in authorizing the warrant. The warrant also was not so facially deficient that the executing officers could not reasonably presume it to be valid. *Clark*, 638 F.3d at 101 ("a warrant is facially defective when it omits or misstates information specifically required to be contained therein"). It specifically identified the account to be searched and the reason for such search.

Khalladi argues only that the good faith exception does not apply because the warrant was so lacking in probable cause as to make reliance upon it unreasonable. Although the Court agrees

that SA Bragg's affidavit failed to establish probable cause, the affidavit was not so lacking in indicia of probable cause "as to preclude reasonable reliance," particularly given the breadth of the conspiracy and the likelihood of finding incriminating evidence in the iCloud account. *Id.* at 103. The affidavit offered some evidence of iPhone use and explained that iCloud accounts often hold a variety of information including iMessages; voicemail messages; call histories; contacts; and other data. Records and data from third-party applications, such as the instant messaging service WhatsApp, can also be backed up on the user's iCloud account. SA Bragg stated that, in his training and experience, evidence of criminal activity may be found in such records and files.

Furthermore, evaluating probable cause in the context of a cloud search can be a complex task. *See, e.g., United States v. McCall*, 84 F.4th 1317 (11th Cir. 2023), *cert. denied*, 144 S. Ct. 1042 (2024). *McCall* found "at the outset that technology moves quickly, the law moves slowly, and the combination can leave law enforcement officers with little insight on how to investigate a cloud account." *Id.* at 1324. "Because courts struggle to decide how probable cause and particularity apply to the information that law enforcement collects from a cloud account, it is unsurprising that police officers might struggle as well." *Id.*

McCall ultimately determined that "the good faith exception applies to close calls and threshold cases." *Id.* (citing *Messerschmidt v. Millender*, 565 U.S. 535, 556 (2012)). As to the broad information available in the cloud account, *McCall* acknowledged that "the warrant required Apple to turn over the entirety of the account's information," and noted its strong preference for a time limitation. *Id.* at 1328. The iCloud warrant in this case provided such a limitation.

As recognized in *McCall*, this is an evolving area of the law. Given that distinction, in addition to the breadth of the alleged conspiracy, the Court finds it was objectively reasonable to rely on the Magistrate Judge's conclusion. *Leon*, 468 U.S. at 921 ("In the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination or his judgment that the form of the warrant is technically sufficient."). The Court therefore declines to apply the exclusionary rule in this instance, and the motion to suppress evidence obtained pursuant to the email and iCloud warrant (ECF No. 51) is denied.

V. 2667 Cell Phone Search

A. Background

After reviewing the iCloud account data, the Government reportedly needed additional location information. It therefore sought CSLI connected to one of Khalladi's phone numbers, ending

in 2667. The Government obtained the 2667 number from Khalladi's American Airlines and Southwest Airlines account information. The airline accounts also showed that he had traveled to Kansas City around the time of suspected episodes of fraud in that city.

SA Bragg's affidavit stated that there was probable cause for the search because "most people have their cell phone on, or near, their person at all times," and

> [c]ell tower location data, associated with the SUBJECT PHONE will assist law enforcement in confirming or denying statement[s] made by the couriers regarding KHALLADI's role in the fraud scheme. Information provided by American Airlines and Southwest Airlines link the SUBJECT PHONE to travel itineraries for KHALLADI. Additionally, a search of KHALLADI's Apple iCloud account further identif[ied] the SUBJECT phone as being used by KHALLADI.

The warrant requested information for the period between March 1, 2022 and December 31, 2023.

B. Analysis

Khalladi contends that nothing in the agent's affidavit connected the 2667 number to the alleged offenses. He also argues that the Government had no reason to believe that a "sophisticated fraudster" would use his personal cell phone for fraud. He submits that the Government could have asserted that a traveler would likely keep the phone associated with an airline account on him while traveling, but that this theory was never articulated in the affidavit.

SA Bragg's affidavit stated that, based on his training and experience, people always have their cell phones on or near them. Standing alone, that statement would fall short of establishing probable cause. As one court recently concluded, "[a]cknowledging that cell phones have become ubiquitous in our society, a finding of probable cause cannot be premised solely on an agent's assertion that most people carry cell phones most of the time." *United States v. Bertini*, No. 23 CR. 61 (PGG), 2023 WL 8258334, at *9 (S.D.N.Y. Nov. 29, 2023). Another recent decision, having surveyed case law within the Second Circuit, noted that "affiants' blanket generalizations about people who commit crimes carrying cell phones, or factually sparse warrant affidavits pertaining to cell phone use, are insufficient to establish particularized, case-specific probable cause. However, factual allegations that tie the phone to the specific crime suffice." *United States v. Rutledge*, No. 23-CR-269 (FB), 2024 WL 1834801, at *3 (E.D.N.Y. Apr. 26, 2024) (cleaned up) (citing *United States v. Baines*, No. 20-CR-00261 (MPS), 2022 WL 35807, at *2, 4 (D. Conn. Jan. 4, 2022) (probable cause existed for CSLI warrant where burglary suspects used their cell phones to "communicate with each other during burglaries" and "to document their exploits during and after burglaries")).

Here, the linchpin for probable cause is the connection between the phone number and the flight itinerary. *See*

Rutledge, 2024 WL 1834801, at *3 (noting "factual allegations that tie the phone to the specific crime suffice"). The phone number was provided to the airlines for contact purposes, and the airline information placed Khalladi in Kansas City near the time of alleged criminal activity in that city. Common sense dictates that when traveling with an airline account, the traveler will retain ready access to the phone number linked to that account in the event the airline sends notifications of flight delays, cancellations, and the like. Consequently, the Magistrate Judge could have reasonably inferred that the 2667 number, and the related CSLI data, would confirm Khalladi's location at that time.

Even if the Court did not find probable cause with respect to the 2667 number, the good faith exception would again apply. As discussed previously, "*Leon* instructs that officers cannot reasonably rely on a warrant issued on the basis of an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Clark*, 638 F.3d at 103 (internal quotations and citations omitted). "Such a concern most frequently arises when affidavits are bare bones, *i.e.*, totally devoid of factual circumstances to support conclusory allegations," and "is particularly acute when facts indicate that the 'bare-bones description ... was almost calculated to mislead.'" *Id.* (alteration in original) (quoting

United States v. Reilly, 76 F.3d 1271, 1280 (2d Cir. 1996), *aff'd on reh'g*, 91 F.3d 331 (2d Cir. 1996)). This case presents no such facts. The supporting affidavit connected the 2667 number to Khalladi's travel in furtherance of the conspiracy, and reliance on the warrant was not unreasonable. The motion to suppress with respect to the 2667 phone warrant (ECF No. 51) is therefore denied.

Conclusion

For the reasons set forth above, Khalladi's pending motions to suppress (ECF Nos. 36, 37, 51) are denied. The related motion to file under seal (ECF No. 52) is granted.

DATED at Burlington, in the District of Vermont, this 10th day of September, 2024.

/s/ William K. Sessions III
Hon. William K. Sessions III
U.S. District Court Judge